(12) **UK Patent Application** (19) **GB** (11) **2 339 121** (13) **A**

(43) Date of A Publication 12.01.2000

(21) Application No 9814003.1	(51) INT CL^7 HO4L 9/22
(22) Date of Filing 30.06.1998	(52) UK CL (Edition R) H4P PDCSP
(71) Applicant(s) Chantilley Corporation Limited (Incorporated in the United Kingdom) 28 Main Street, Mursley, MILTON KEYNES, Bucks, MK17 0RT, United Kingdom	(56) Documents Cited GB 2301266 A
(72) Inventor(s) William McMullan Hawthorne	(58) Field of Search UK CL (Edition Q) H4P PDCSP INT CL^6 HO4L 9/12 9/18 9/22 9/26 ONLINE DATABASES: WPI, EPODOC, JAPIO
(74) Agent and/or Address for Service Urquhart-Dykes & Lord Three Trinity Court, 21-27 Newport Road, CARDIFF, CF24 0AA, United Kingdom	

(54) Abstract Title
Apparatus for generating a session key to encrypt or decrypt messages

(57) An apparatus for encrypting and decrypting messages is arranged to randomly generate a session key of a variable selected number of characters. The randomly generated characters are distributed in sequence into a predetermined number of groups (in the same manner as dealing a pack of cards out) to form a set of primitives. Successive pairs of primitives are combined in a XOR procedure and a successive multiple of 100 is added to each result. The primitives thus produced are used in accordance with a predetermined algorithm to form a cypher key stream for encrypting or decrypting successive characters of a message. The apparatus is for use in a facsimile machine.

GB 2 339 121 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

The claims were filed later than the filing date but within the period prescribed by Rule 25(1) of the Patents Rules 1995.
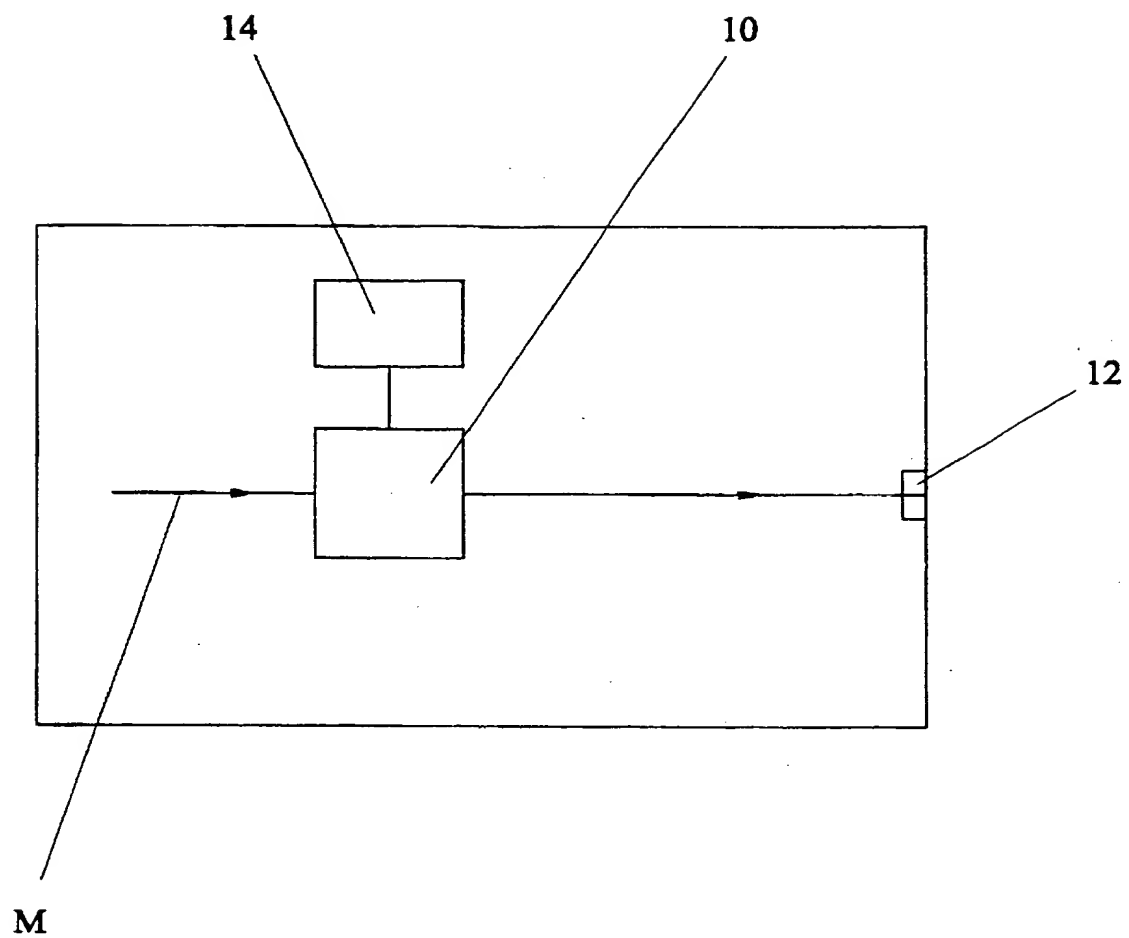
14

10

12

M

FIG.   1

(1) Randomly generated 56 figures secret key .....
44490925319354895003213478116711124821791736922366044359 = 186 bits

```
4863  4976  4519  9012   0012   9323   2246   5186   3320   1414   9774   3893   5515   4179
4863  399   4136  13084  13072  6011   8125   3071   1799   641    9391   11162  14433  10290
4963  599   4436  13848  13572  6611   8825   3171   1999   941    9791   11662  15033  10990
```

(2) Randomly generated 48 figure secret key .....
019301259141828933881545855137151100195663513916 = 159 bits

```
0835  1971  9313  3359   0811   1816   210    550    941    159    485    156    856    213
835   1264  8337  11662  11941  10685  10607  11081  10468  10363  10654  10498  10842  10895
935   1464  8637  12062  12441  11285  11307  11181  10668  10663  11054  10998  11442  11595
```

(3) Randomly generated 40 figure secret key .....
8272611489892272004839562205012958050601 = 133 bits

```
870  221   702  209  645   188   130   495  850  966  820  921   20    25
870  955   261  468  849   1005  879   640  466  532  288  697   685   692
970  1155  561  868  1349  1605  1579  740  666  832  688  1197  1285  1392
```

(4) Randomly generated 32 figure secret key .....
71936502524388145097469032024067 = 106 bits

```
714  140  956  307  69   57   04   26   59   20   43   32   80   82
714  582  506  201  140  181  177  171  144  132  175  143  223  141
814  782  806  601  640  781  877  271  344  432  575  643  823  841
```

(5) Randomly generated 18 figure secret key .....
241895746918348060 = 60 bits

```
20   40   16   80   9    5    7    2    4    1    8    3    4
28   52   36   116  125  120  127  123  116  117  125  126  122
128  252  336  516  625  720  827  223  416  517  625  726  822
```

(6) Randomly generated 12 figure secret key .....
449078277840 = 40 bits

```
4    4    9    0    7    8    2    7    4    8    4    0    4    4
4    0    9    9    14   6    4    3    8    12   8    8    12   8
104  200  309  409  514  606  704  103  204  312  408  508  612  708
```

FIG. 2

ENCRYPTION AND DECRYPTION KEY ARRANGEMENTS

The present invention relates to apparatus arranged to encrypt messages or decrypt messages, particularly to communications apparatus arranged to encrypt messages prior to transmission and decrypt received messages.

5   It is known to provide communications apparatus (for example facsimile machines) with the ability to encrypt messages prior to transmission and decrypt received messages. However, each such apparatus operates with a cypher of a predetermined, fixed cryptographic strength: two apparatus can
10   only communicate with each other if they both use cyphers of the same strength. There are many circumstances in which this limits the ability for communications to be established.

We have now devised an arrangement in which the cypher can be varied in strength, so that when any two apparatus wish
15   to communicate with each other, a common cypher strength can be selected.

Thus, in accordance with the present invention, there is provided an apparatus which is arranged to encrypt or decrypt messages, the apparatus being arranged to generate a
20   session key of a variable selected number of characters and to distribute the characters of said session key in sequence into a predetermined number of groups to form a corresponding predetermined number of primitives, and further arranged to use said primitives, in accordance with a predetermined algorithm,
25   to form a cypher key stream the characters of which are used in sequence to encrypt or decrypt successive characters (or other elements) of a message.

In use of this apparatus, the length (i.e. the number of characters) of the session key can be selected: the longer
30   the session key, the greater will be the strength of the cypher.

Once the length of the session key to be used is decided upon, the session key is preferably randomly generated.

Preferably the characters (typically numerical
35   characters) of the session key are distributed into the predetermined number of groups in a manner forming a

corresponding set of multi-digit numbers. For example, the first term allocated to each group may form the first digit of a multi-digit number, the second term allocated to that group forms the second digit of the multi-digit number, and so on.

5   Preferably these multi-digit numbers are processed further in order to produce the corresponding set of primitives, used to form the cypher key stream.

Preferably successive pairs of these multi-digit numbers are then subjected to an XOR (exclusive OR) process to
10 form a corresponding set of results.

Preferably predetermined values are then added to the respective results of the XOR process, to form a corresponding set of primitives. Preferably different values are added to the different results of the XOR process: preferably these
15 different values are different multiples of a basic value. For example, 100 may be added to the first XOR result, 200 to the second, and so on.

An embodiment of the present invention will now be described with reference to the accompanying drawings, in
20 which:

FIGURE 1 is a schematic block diagram showing part of the electronic system of communications apparatus in accordance with the present invention; and

FIGURE 2 is a table showing the formation of six
25 different groups of primitives from six session keys of different lengths.

Referring to Figure 1, a communications apparatus (e.g. a facsimile machine) comprises means 10, in the form of a microprocessor, for encrypting a plain message M prior to
30 transmission via a port 12. The microprocessor 10 is provided with a program memory 14 which stores an encryption algorithm and also an algorithm for forming a group of primitives from a session key. The microprocessor is able to generate a session key on a random basis, of selected length. The
35 microprocessor is also arranged to correspondingly decrypt messages received via the port 12.

In effecting communication between two apparatus, these follow an initial protocol to determine the cryptographic strength to be employed: this determines the length of the

session key to be used. Then the session key is randomly generated by the microprocessor 10 in one of the apparatus: Figure 2 shows six different examples, in which session keys of 56,48,40,32,18 and 12 decimal digits (186,159,133,106,60 and
5 40 binary bits) are generated.

Once the session key of selected length has been generated, the microprocessor distributes its digits, one-after-another, into 14 groups, in the same manner as dealing a pack of cards out to the players of a card game. Thus,
10 referring to the first example in Figure 2, the first 14 digits (44490925319354) form the first digits of respective 4-digit numbers: continuing, the next 14 digits of the session key (89500321347811) form the second digits of the respective 4-digit numbers, the next 14 digits of the session key
15 (67111248217917) form the third digits of the respective 4-digit numbers and the final 14 digits of the session key (36922366044359) form the fourth (and final) digits of the respective 4-digit numbers. In the first example in Figure 2, 14 groups of 4-digit numbers are thus formed: however, in each
20 of the other examples, the number of digits in the session key is not divisible by the number of groups (14), so that 14 numbers of differing numbers of digits are formed (in some cases, only a single digit).

In the next step, the microprocessor 10 combines
25 successive pairs of the 14 numbers in an XOR (exclusive OR) procedure: in each of the examples shown in Figure 2, the second line gives the corresponding results. In particular, each number in the first line is combined with the XOR result of the proceeding number, in a process which involves an XOR
30 function or their binary equivalents.

In the next step (third line of each example shown in Figure 2), the microprocessor 10 adds a multiple of 100 to each of the 14 results formed by the XOR procedure. Thus, to the first result, 100 is added: to the second result, 200 is
35 added; to the third result, 300 is added, and so on up to the seventh result, to which 700 is added. Then, to the eighth result, 100 is added: to the ninth result, 200 is added, and so on up to the fourteenth result, to which 700 is added. The final results (last line in each of the 6 examples set out in

Figure 2) provide a set of 14 primitives.

It will be appreciated that the second and third steps which have been described add complexity to the primitives finally produced. The third step in particular ensures that
5 none of the primitives will be zero.

The 14 primitives thus produced are used by the microprocessor, in accordance with the encryption algorithm, to form a cypher key stream comprising a long stream of digits. Then, in order to encrypt a plain message, the digits of this
10 stream are taken one-after-another, and used in accordance with an encryption algorithm to encrypt respective, successive elements (e.g. characters or groups of characters) of the message to be transmitted. Similarly, in order to decrypt a received message, the digits of the cypher key stream are taken
15 one-after-another and used, in accordance with a decryption algorithm (being the inverse of the encryption algorithm) to decrypt respective, successive elements of the received message.

Claims

1)   An apparatus which is arranged to encrypt or decrypt messages, the apparatus being arranged to generate a session key of a variable selected number of characters and to
5   distribute the characters of said session key in sequence into a predetermined number of groups to form a corresponding predetermined number of primitives, and further arranged to use said primitives, in accordance with a predetermined algorithm, to form a cypher key stream the characters of which are used
10 in sequence to encrypt or decrypt successive characters (or other elements) of a message.

2)   An apparatus as claimed in claim 1, arranged to generate said session key in random manner.

3)   An apparatus as claimed in claim 1 or 2, arranged so
15 that the characters of the session key are distributed into said predetermined number of groups in a manner forming a corresponding set of multi-digit numbers.

4)   An apparatus as claimed in claim 3, arranged to further process said multi-digit numbers to produce said primitives.

20 5)   An apparatus as claimed in claim 4, arranged to subject successive pairs of said multi-digit numbers to an exclusive OR process to form a corresponding set of results, and to process said results to produce said primitives.

6)   An apparatus as claimed in claim 5, arranged so to add
25 predetermined values to the respective said results, to form said primitives.

7)   An apparatus as claimed in claim 6, arranged to add different said values to different said results.

8)   An apparatus as claimed in claim 7, arranged such that
30 said different values are different multiples of a basic value.

9)   An apparatus which is arranged to encrypt or decrypt messages, the apparatus being substantially as herein described with reference to the accompanying drawings.

INVESTOR IN PEOPLE

| Application No: | GB 9814003.1 | Examiner: | Gareth Griffiths |
| Claims searched: | All | Date of search: | 13 August 1999 |

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

  UK Cl (Ed.Q): H4P (PDCSP)

  Int Cl (Ed.6): H04L 9/12, 9/18, 9/22, 9/26

Other: Online Databases: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A	GB2301266 A (WILLIAM YIN SHAW)	